A few charts

New England Conference of Public Utilities Commissioners

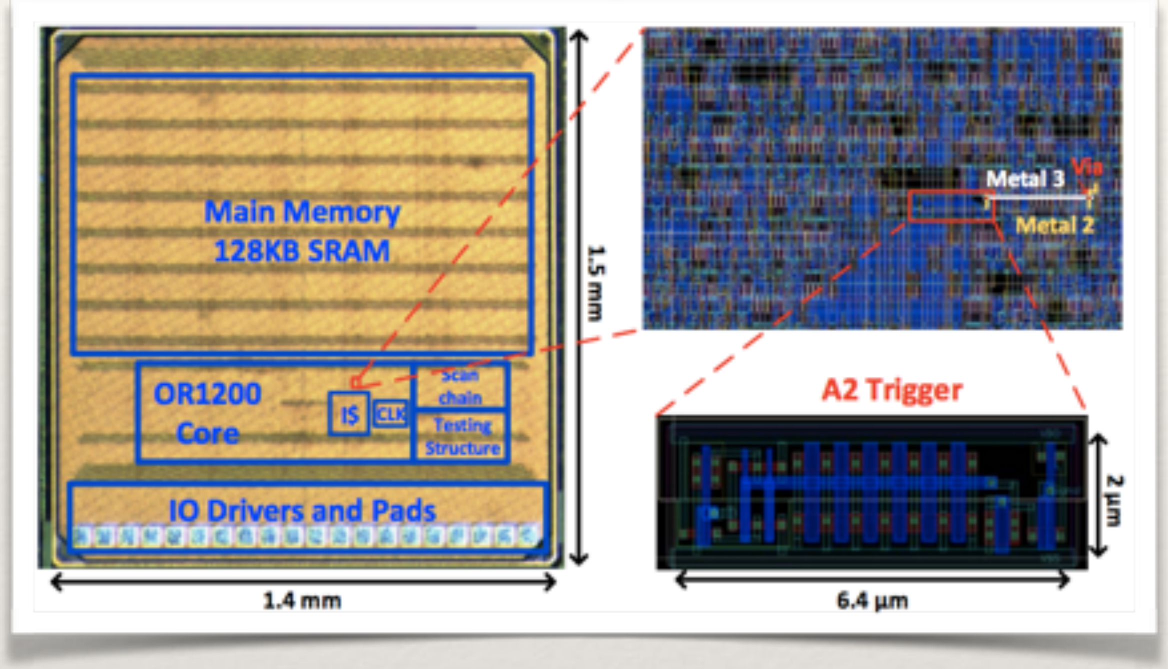
Addressing Cybersecurity in the 21st Century

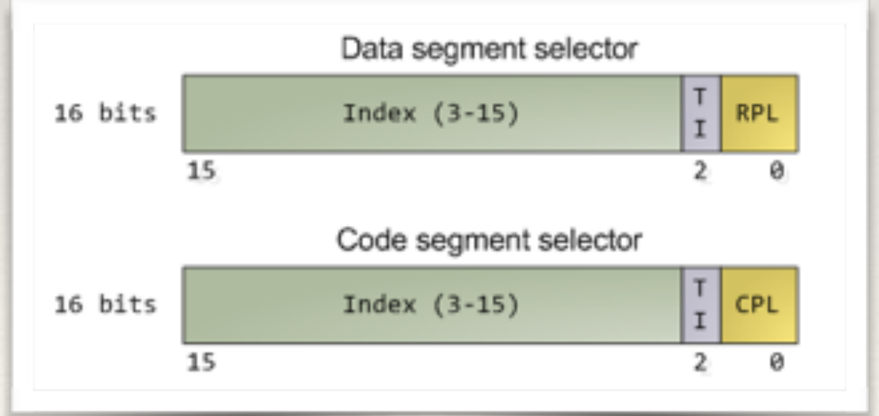
Chris Spirito
Mission Support Center

christopher.spirito@inl.gov

Cyber related Threats

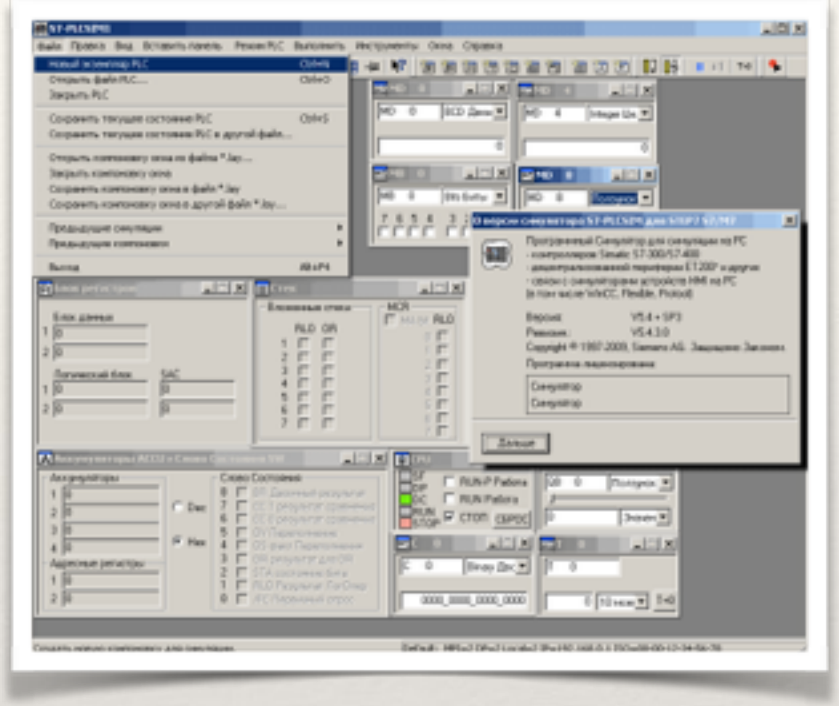
Sophisticated Design and Fabrication Time Attacks





CPU tracking of Current Privilege Level (CPL)

The Art of the Possible and IRONGATE



PLCSIM

IRONGATE Malicious Concepts

Deceptive Man-in-the-Middle {PLC Broker}

Sandbox Evasion {VMware | Cuckoo}

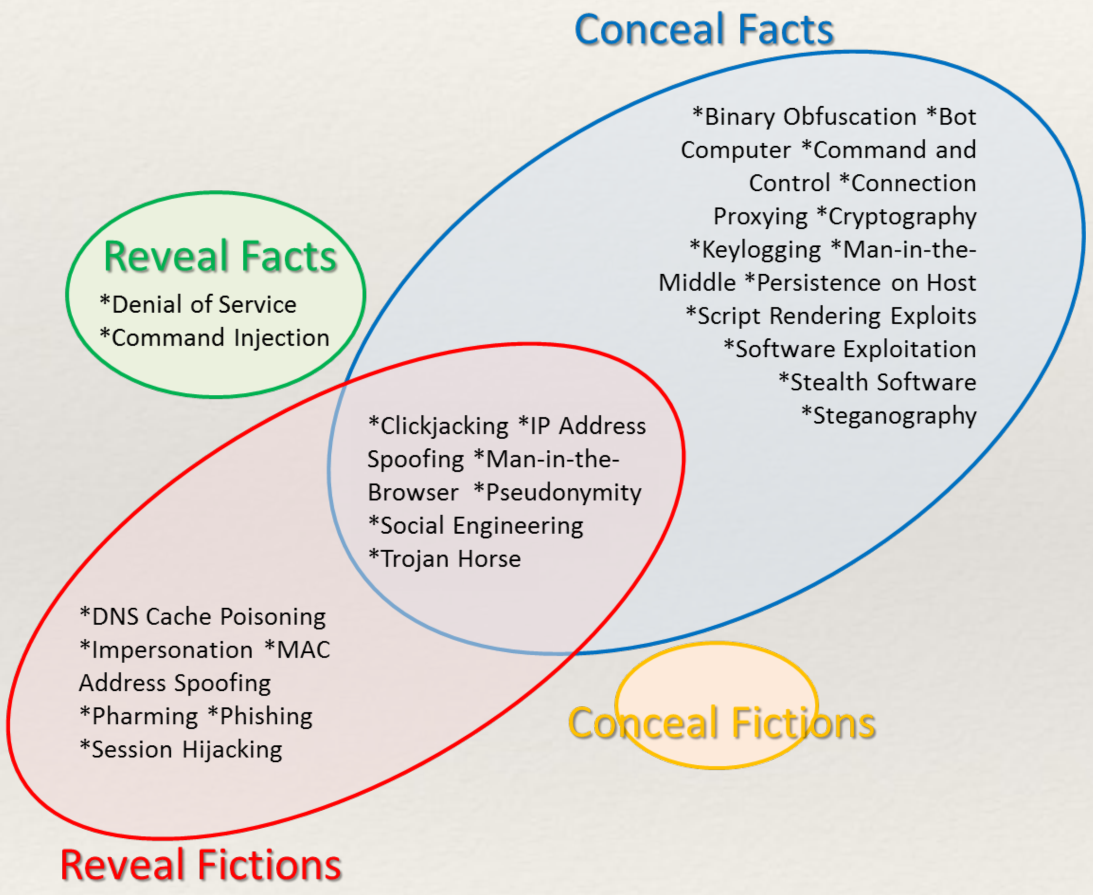
Dropper Observables {Compiled with PyInstaller}

IRONGATE: http://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

A2: Analog Malicious Hardware: http://ieee-security.org/TC/SP2016/papers/0824a018.pdf

Blended Attacks and Campaigns

Attacker Denial and Deception TTPs



Conceal Facts

*Binary Obfuscation *Bot Computer *Command and Control *Connection Proxying *Cryptography *Keylogging *Man-in-the-Middle *Persistence on Host *Script Rendering Exploits *Software Exploitation *Stealth Software *Steganography

Reveal Facts

*Denial of Service
*Command Injection

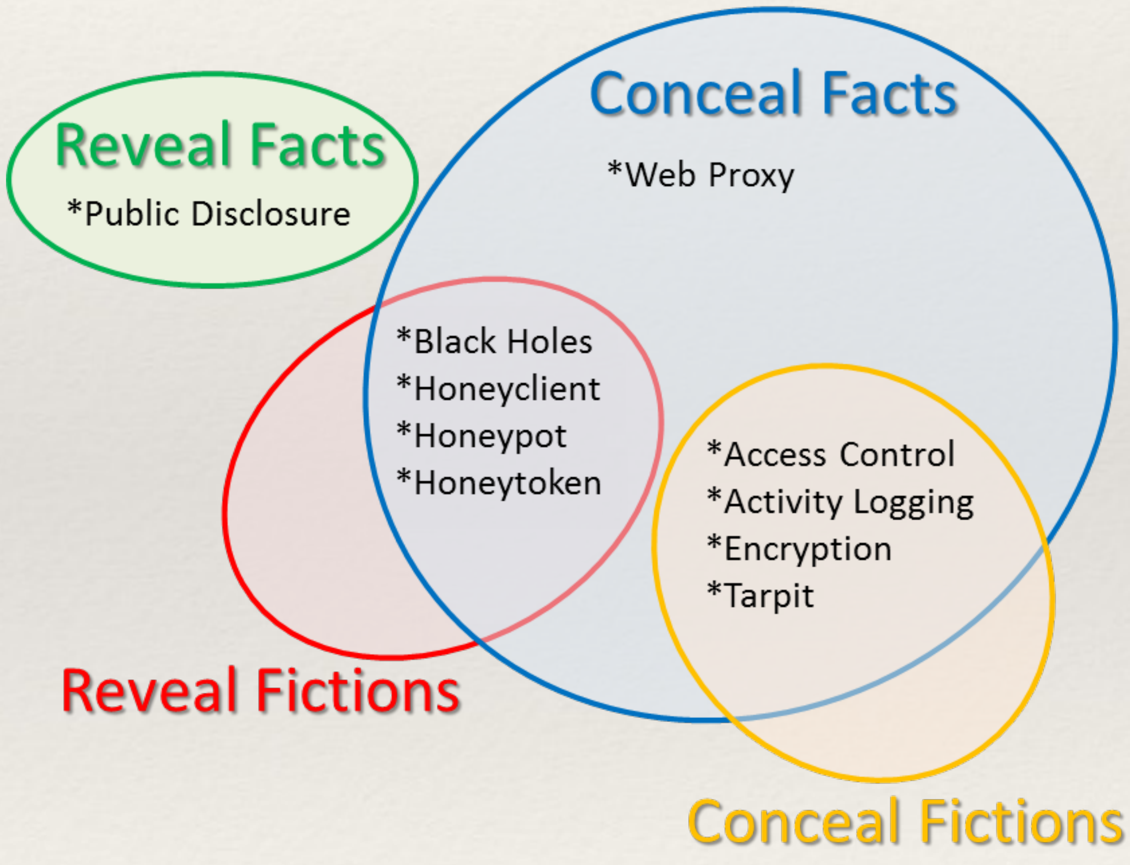
*Clickjacking *IP Address Spoofing *Man-in-the-Browser *Pseudonymity *Social Engineering *Trojan Horse

*DNS Cache Poisoning *Impersonation *MAC Address Spoofing *Pharming *Phishing *Session Hijacking

Conceal Fictions

Reveal Fictions

Defender Denial and Deception TTPs



Reveal Facts

*Public Disclosure

Conceal Facts

*Web Proxy

*Black Holes
*Honeyclient
*Honeypot
*Honeytoken

*Access Control
*Activity Logging
*Encryption
*Tarpit

Reveal Fictions

Conceal Fictions

Cyber Denial, Deception and Counter Deception: http://www.springer.com/us/book/9783319251318

Working Group on the Future of US-Russia Relations

Sergei Karaganov
Dean, School of World Economy and International Affairs, National Research University – Higher School of Economics; Honorary Chairman of the Presidium, Council on Foreign and Defense Policy (CFDP); Russian co-chair of the Working Group

Tim Colton
Morris and Anna Feldberg Professor of Government and Russian Studies and Chair, Department of Government, Harvard University; Executive Committee Member, Davis Center for Russian and Eurasian Studies, Harvard University, US Co-chair of the Working Group

Fyodor Lukyanov
Chairman of the Presidium, Council on Foreign and Defense Policy; Editor in Chief, *Russia in Global Affairs* Journal

Alexandra Vacroux
Executive Director, Davis Center for Russian and Eurasian Studies, Harvard University

Toward U.S.-Russian Bilateral Cooperation in the Sphere of Cybersecurity

Christopher Spirito
US DoE - INL

Tom Remington
Emory University

Oleg Demidov
PIR Center

Vitaly Kabernik
PIR Center

Elena Chernenko
Kommersant

Recommendations

- Explicit definition of thresholds for attacks on critical infrastructure should be established.
- Agreement on types of information to share in the event of an attack should be set.
- Prohibition on automatic retaliation.
- Prohibition on attacks against another nation's Internet infrastructure
- Joint Internet Governance
- Broader International Discussion within the UN GGE

Questions Raised

- Will there ever be a full out cyber war between the US, Russia and China?
- What is a cyber weapon and how is it used?
- What should society do about subversion/exploitation of trusted platforms?
- What strategic advantage is gained through the use of cyber capabilities?